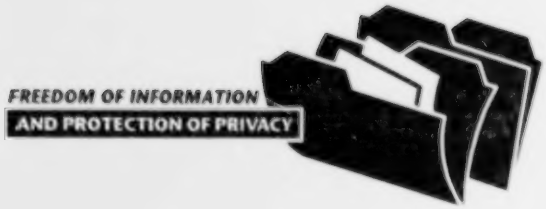

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY

Contract Manager's Guide

December 2003

ISBN 0-7785-3106-6

Alberta
GOVERNMENT OF ALBERTA

Information Management, Access and Privacy
Alberta Government Services
3rd Floor, 10155 – 102 Street
Edmonton, Alberta
Canada, T5J 4L4
Phone: (780) 422-2657
Fax: (780) 427-1120
Web sites: www.gov.ab.ca/foip
www.psp.gov.ab.ca
www.im.gov.ab.ca

FOIP Help Desk: (780) 427-5848
Toll free dial 310-0000 first
E-mail: foiphelpdesk@gov.ab.ca

For more information on Alberta's FOIP legislation, see:

Freedom of Information and Protection of Privacy web site: www.gov.ab.ca/foip
Publications, including:

- *The Right to Information and the Right to Privacy* brochure
- *FOIP: A Guide*
- *FOIP Guidelines and Practices*
- *FOIP News*
- *Contractors' Guide to the FOIP Act brochure*
- *Contract Manager's Guide*
- *Conducting Surveys: A Guide to Privacy Protection*
- *Guide for Developing Personal Information Sharing Agreements*
- *Guide to Developing Privacy Statements for Government of Alberta Web Sites*
- *Guide to Using Surveillance Cameras in Public Areas*
- *Guide to Providing Counselling Services in School Jurisdictions*
- *Human Resources Guide for Local Public Bodies*
- *Using and Disclosing Personal Information in School Jurisdictions*
- Legislation
- FOIP Coordinators/Contacts
- Information and Privacy Commissioner's Orders and Investigation Reports
- Frequently Asked Questions

Queen's Printer
Edmonton: (780) 427-4952
Calgary: (403) 297-6251
Toll free by dialing 310-0000 first
Web site: www.qp.gov.ab.ca

- *FOIP Act and Regulation*
- *FOIP Guidelines and Practices*
- *Annotated FOIP Act*

Office of the Information and Privacy Commissioner
410, 9925 - 109 Street
Edmonton, Alberta T5K 2J8
Phone: (780) 422-6860 (toll free dial 310-0000 first)
Toll Free: 1-888-878-4044
Fax: (780) 422-5682
E-mail: generalinfo@oipc.ab.ca
Web site: www.oipc.ab.ca

INTRODUCTION

This guide has been prepared to help contract managers in public bodies of the Government of Alberta ensure their organizations are in compliance with the *Freedom of Information and Protection of Privacy (FOIP) Act* and the Records Management Regulation. It contains information that contract managers need in order to deal effectively with:

- access to information, protection of privacy and records management issues throughout the life cycle of the contract; and
- requests for access to records created in the contracting process.

Alternative methods of service delivery – outsourcing of information technology (IT) services, joint service delivery and privatization – all involve additional considerations for the public body in meeting its obligations under the FOIP Act. Because of this, this guide also includes additional information for assessing risk and methods that might be used to ensure compliance with the Act.

You can get additional information on access to information and protection of privacy issues from your public body's FOIP Coordinator. As well, Information Management , Access and Privacy of Alberta Government Services regularly publishes bulletins and other guidelines on the application of the FOIP Act. This information is available on the FOIP web site at www.gov.ab.ca/foip. Your Senior Records Officer (SRO) can also advise you on records management issues.

While the Guide is written for a government audience, local public bodies subject to the FOIP Act can draw from the contracting process and considerations described in this document.

NOTE: This guide does not provide legal advice. The sample contract clauses provide suggested examples only. You should always obtain legal advice on contract wording and other issues when establishing a specific contract.

Freedom of Information and Protection of Privacy
Contract Manager's Guide

Table of Contents

Chapter 1: Contracts and FOIP 1
1.1 Introduction 1
1.2 Custody and Control of Records 1
1.3 Effect on Contracting 3

Chapter 2: Alternative Service Delivery 4
2.1 Outsourcing 4
2.2 Joint Service Delivery 9
2.3 Privatization 10

Chapter 3: The RFP and Tendering Process 13
3.1 Requests for Proposals 13
3.2 Communicating Requirements to Contractors 13
3.3 Complying with FOIP 15

Chapter 4: Negotiating and Managing the Contract 17
4.1 Drafting the Contract 17
4.2 Records Management 17
4.3 Access to Information 21
4.4 Protection of Privacy 22
4.5 Hold Harmless 26
4.6 Monitoring Compliance 26
Table 1 Methods of Dealing with Risk 27

Appendix 1 Glossary of Terms 28
Appendix 2 Checklist for Contract Managers 30
Appendix 3 Releasing Contracting Records in Response to a FOIP Request . 33
Appendix 4 Disclosure of Documents used in Contracting 40
Appendix 5 Records Management Regulation 41

Chapter 1
Contracts and FOIP

1.1 INTRODUCTION

Alberta Government departments, agencies and other provincial public bodies routinely use a variety of contracts to obtain goods and services as well as to implement new ways of providing service delivery. This Guide is designed to assist contract managers to determine how the *Freedom of Information and Protection of Privacy (FOIP) Act* and the Records Management Regulation (RMR) established under the *Government Organization Act* affect the contracting process and to provide guidance on implementation.

Chapter 1 discusses which records are subject to the FOIP Act and RMR and how contractors may also be required to adhere to the requirements of the Act and regulation. If the Act and regulation apply, contractors must be made aware of how they will apply in the RFP and tendering process (discussed in Chapter 3) and the specific requirements must be set out in the contract (discussed in Chapter 4.)

The majority of government contracting is simply to obtain goods and services for government use. Such contracting often does not require the contractor to handle government information or to deal with personal information. In these cases, consideration of the requirements of the FOIP Act and the RMR will likely be marginal.

In such cases, you should focus on the requirements of the RFP and tendering process discussed in Chapter 3. To determine the extent to which the FOIP Act or the RMR will affect the particular contract under consideration, you may find it helpful to review the Checklist in Appendix 2. This may assist in focussing how this Guide will apply in each situation.

When contracts involve services dealing with personal information, or with outsourcing, joint service delivery or privatization of government programs, there are many factors that you must consider. These factors are discussed in Chapter 2. In general, the remainder of this Guide offers specific suggestions for tendering and contract clauses.

It is the policy of the Government of Alberta that its departments, agencies, boards, and commissions (collectively referred to as "public bodies") take access to information, protection of privacy and records management requirements into account when considering these types of contracts.

1.2 CUSTODY AND CONTROL OF RECORDS

The legal obligations regarding access to information, protection of privacy and records management are based on the concepts of *custody* and *control* of records. The FOIP Act applies to all records in the *custody* or under the *control* of a public body, except for those records for which there is a specific exclusion in **section 4** of the FOIP Act. The RMR also applies to all

records that are in the custody or under the control of a public body.

A public body would have control of records produced specifically for a contract. This could include records transferred to a contractor or records created, obtained or maintained by a contractor. Therefore, a contract will have to specify a number of conditions to address the access and privacy provisions of the FOIP Act relating to the management of these records.

What is Meant by Custody or Control?

A public body has *custody* of a record when the record is in the possession of the public body.

A record is under the *control* of a public body when the public body has the authority to manage the record, including restricting, regulating and administering its use, disclosure or disposition.

Does the Public Body Have Custody or Control?

In many contracting situations, records will be created or maintained by the contractor, but remain under the control of the public body. In some cases, information may be transferred to the contractor, but remain in the custody or under the control of the public body.

The following factors will help you in deciding whether the records created in a contracting situation are in the custody or under the control of the public body. These questions are by no means an exhaustive list of all factors that should be considered.

- Does information collected or created under the contract have to be maintained as records under the RMR or another enactment?
- Were the records created by a contracted consultant for the public body?
- Have the records only been physically or electronically transferred to the contractor but remain the property of the Crown?
- Is the public body bound by its own legislation to maintain the types of records required by the contract, or are there other requirements to maintain the records (e.g., requirements imposed by the Auditor General, or for law enforcement)?
- Does the public body need to create and maintain specific records that it can access either during or beyond the life of the contract?
- Does the contract permit the public body to inspect, review or copy records produced, received or acquired by a contractor as a result of the contract?
- Does the public body have the authority to regulate use of the records?
- Does the public body have authority to dispose of the records?
- Who has copyright in the records?

For example, a public body may have a contract in place for providing particular services to individuals. If the contract requires the contractor to make records available to the public body to audit services provided, the records used by the public body to monitor or inspect the delivery of the services would likely be under its control.Similarly, if a counsellor under contract to a public body maintains notes of his or her

counselling activities, these notes may be under the control of the public body.

As long as records are in the custody or under the control of a provincial public body, the legal requirements of the FOIP Act and the RMR apply.

After January 1, 2004 individuals will be able to access personal information about themselves from the contractor under Alberta's *Personal Information Protection Act*, unless public bodies have retained control of the records containing personal information.

1.3 EFFECT ON CONTRACTING

The type of contract you are developing determines how you handle access to information, protection of privacy and records management. For example, in a simple contract to purchase goods, such as a standing offer for office supplies, there are few issues related to FOIP and records management. The records created during the contract (e.g., invoices, purchase orders) will remain in the custody and under the control of the public body.

The situation becomes more complex, though, for contracts to carry out a service on behalf of the public body and contracts where personal information is collected, used or disclosed (e.g., development of a training program, a customer survey or alternative program delivery).

In these cases, you will need to consider many of the following issues:

- conditions regarding custody and control of records;
- access to the information;
- copyright;
- the types of information and records the contractor is expected to collect or create and maintain under the contract;
- the conditions or standards for maintaining these records;
- the locations of active and stored records;
- the records retention period and conditions governing the disposition of records;
- the disposal or destruction of records;
- the confidentiality of information received or compiled;
- security;
- protection of personal information; and
- the ability to retrieve records to respond to FOIP requests.

In the following sections of this Guide, these issues are discussed in more detail as they relate to the Request for Proposal (RFP) and tendering process, the contract itself, and ongoing management of the contract. Additional considerations for special cases such as information technology outsourcing agreements, joint service delivery, and privatization are also discussed.

Chapter 2
Alternative Service Delivery

2.1 OUTSOURCING

Outsourcing is a common method of service delivery used by public bodies. All or a significant part of a service previously delivered by government may be delivered by another level of government, a non-profit organization or by the private sector. The service provider is paid a contracted sum for providing the service and assumes the overhead and other costs associated with service delivery.

This approach has been used for the delivery of information technology (IT) services and is expanding into a broad range of operational areas, from health, safety and technical inspections to the operation of programs or facilities.

Outsourcing agreements often mean that information under the control of the public body is stored and processed off-site and by a separate entity. As a result, such contracts are usually more detailed and complex and require more attention, especially with regard to records management and, if personal information is involved, the protection of privacy.

The FOIP Act and the RMR apply to all the records under the custody or control of the public body that are transferred, created, obtained and/or maintained as a result of an outsourcing activity. All outsourcing contracts dealing with the delivery of government services where the government maintains custody or control of the records should contain:

- A section on *records management* that deals at an appropriate level of detail with the nature of the records under the government's custody or control, the ownership of those records and standards relating to their management and disposition. This includes approval of records retention and disposition schedules for such records by the Alberta Records Management Committee. Records management standards, with the exception of the requirement to develop a records retention and disposition schedule for the records, may either reflect the records management standards of the public body or special standards developed for the contract or agreement.
- A section on *access to information* that indicates that the applicable records identified under the government's custody or control are governed by the access provisions of the FOIP Act and assigns responsibilities and standards for responding to FOIP requests.
- For personal information that remains under the custody or control of the government, a section on the *protection of privacy* that establishes standards for the protection of personal information. These standards must meet the requirements of **Part 2** of the FOIP Act.

Assessing Risk

The government's Contract Framework for Information Technology Projects[1] identifies the need for government departments to assess the risks of such contracts at various stages of the process – when deciding to outsource, developing the RFP, and managing outsourcing contracts.

IT outsourcing contracts vary considerably. This section only summarizes the key areas of risk associated with IT outsourcing.[2] While many of the risks identified may relate to more general business risks associated with IT outsourcing, the focus here is on risks directly related to the public body's ability to meet its obligations under the FOIP Act and the RMR. These risks can be considered under the following categories:

- collection and use,
- maintaining custody and control,
- data storage and right of access,
- security,
- destruction of records,
- risk associated with special types of information, and
- monitoring compliance.

For the purpose of this discussion, no distinction is made between contracts that provide for outsourcing of data processing functions and contracts that involve the outsourcing of services flowing from those functions. Public bodies will need to assess the level of risk depending on the scope of the outsourcing arrangement.

Collection and Use

The FOIP Act specifies the purposes for which personal information may be collected and used.

There is a possibility that personal information may be collected by the provider of outsourced services for purposes that are not authorized by the Act. Also, there is a risk that personal information may be used for purposes other than for which it was initially collected.

The public body should specify conditions for collecting and using personal information. In some cases, training and education for the service provider's staff with respect to FOIP may be required. If so, this requirement should be included in the contract.

Maintaining Custody and Control

There are a number of risks associated with the ability of the public body to ensure its ability to maintain custody and control of the records if that is required. These risks relate to:

- **Media Format**
  Are the records stored in a medium that is generally available from other providers? If not, the public body risks not being able to change providers should the need arise.

- **Data and File Specifications**
  Are records and file specifications

---

[1] This publication is available from Innovation and Science or on the following web site: www.gov.ab.ca/cio

[2] A more complete discussion of risks associated with IT outsourcing is contained in the Contract Framework for Information Technology Projects referred to above.

clearly documented so that the data can be converted, if need be, in the future?

- **Compression and Encryption**
  Are data compression and encryption methods and standards clearly documented so that information can be easily recovered?

- **Disaster Recovery and Business Continuity**
  Are disaster recovery procedures in place, including off-site storage of backups? Are procedures in place for alternative methods of service delivery in the event of an unforeseen disruption to business?

- **Transfer when the Contract Ends**
  Are there clear procedures to retrieve the records when the contract ends?

To deal with these risks, the public body should consider:

- specifying standards and documentation requirements for media format, data and file specification, compression and encryption;
- specifying the method and timing of backup, off-site storage and disaster recovery, and the requirement for a business continuity plan; and
- developing clear procedures for the transfer of data when the contract ends.

Data Storage and Right of Access

Closely related to the ability to maintain custody and control are risks associated with record storage. These risks relate to the physical location of the records, segregating the information, transfer to third parties and rights of access.

- **Physical Location**
  Does the public body know the precise location of record storage? Are records stored in a single location or multiple locations? If records are stored in multiple locations, risks of access and recovery become more complicated.

  If the records are to be stored outside of Canada, there are increased risks associated with the possibility that the law in the other country may require the recipient of the records, in certain circumstances, to disclose personal information to the state. These legal requirements might take precedence over any contract to which the provider is party.

- **Segregation**
  Are the public body's records stored together with the records of other customers without description labels? If your records are not segregated, there is a risk that the provider may have difficulty meeting the right of access for the department without compromising its ability to preserve and protect the property of other customers on the premises.

- **Transfer to Third Parties**
  Does the contractor have the right to transfer records to third parties (e.g., subcontractors)? Does this transfer relieve the contractor of obligations under the contract? Does the department have a right of refusal for third-party transfers? Transfers to third parties should include a

means of binding the third party to the same standards as the contractor.

- **Right of Access**
  Even though the location of data storage may be known, it is important to assess the risks associated with the right of access. For example, what if the contractor stores data on leased premises and fails to pay the rent or ceases to carry on business? Is the public body able to recover data if the landlord denies entry to the premises? While an irrevocable right of entry to leased storage premises may be granted by a landlord, there is a risk that this right might not be honoured by a new landlord should the premises be sold or transferred. This added risk may require that the irrevocable right of entry be registered on the title to the property.

  Finally, the right of access goes beyond access by the public body to data under its custody and control. Under the FOIP Act, individuals have a right to access their personal information. Engaging an external contractor, but failing to maintain an absolute right of access to the associated records may mean that the department cannot fulfil its legal responsibility to provide individuals with access to their information upon request.

Some of the methods the department may use to reduce the risks associated with record storage and right of access are:

- require notification of physical location of data storage;
- limit storage to a single location;
- define requirements for the segregation of data;
- ensure the right of access;
- negotiate an irrevocable right of access;
- assess the financial viability of the service provider;
- limit the right of transfer to third-party providers; and
- ensure a process for individuals to exercise their right to access personal information.

Security

There are potential risks related to maintaining the confidentiality and security of the information. Does the contractor have adequate technical and organizational security measures in place to make sure that there is no unauthorized access to the information?

The contract manager should define technical security requirements as well as any organizational security requirements (e.g., who has access to the computer system, files, and stored records) in the outsourcing RFP and any resulting contract.

Destruction of Records

The government Records Management Regulation governs the disposition of records by public bodies. Are retention schedules and policies related to retention and disposition of records clear and understood by the external service provider? Is there adequate protection against the inadvertent or improper destruction of records?

Outsourcing agreements should include retention schedules and policies related to the destruction of records, and should ensure that there are adequate recovery methods if records have been inadvertently destroyed.

Risks Associated with Special Types of Information

The *Freedom of Information and Protection of Privacy Act* does not create classes of personal information. This means that all personal information must be safeguarded.

The contract manager should consider the potential damage that may be caused by a breach of contract (e.g., a breach in confidentiality or security or methods of collecting information covered by the contract), should one occur.

Specifically, there may be types of information where the damage caused by a breach of privacy protection would be severe and therefore represents an increased risk. Some examples of this are:

- services that carry a risk of financial loss to the individual (e.g., credit card payments over the Internet);
- cases where there may be a risk to personal safety if information is improperly disclosed (e.g., victims of crime);
- information which could significantly affect the individual (e.g., hiring, promoting, granting of credit);
- information that could damage the individual's reputation (e.g., unsubstantiated complaints);
- cases where unauthorized disclosure or use may result in an intrusion into an individual's private life (e.g., unsolicited telephone calls);
- agreements involving collecting data in a particularly covert or clandestine manner (e.g., use of Internet cookies); or
- services involving sensitive categories of data (e.g., health information).

The contract manager should identify any special needs (e.g., enhanced security procedures) related to highly sensitive information.

Monitoring Compliance

Finally, there are risks relating to compliance – that is, how the public body knows whether the requirements of the FOIP Act are being complied with during the period of an outsourcing agreement. If there are no monitoring clauses (e.g., on-site visits, audits, reporting requirements) in the agreement, the risk of assessing non-compliance increases and the public body may only discover non-compliance once a problem occurs.

The contract manager should consider:

- establishing regular compliance reporting,
- establishing the right to monitor or audit the contractor, and
- requiring FOIP training for staff of the contractor.

The degree of risk will vary widely depending on the scope of the outsourcing agreement and the type of information involved. However, risk can be reduced through adequate management of the contracting process

(the RFP, contract negotiations, and ongoing management of the contract).

Table 1 summarizes steps that contract managers should consider at various stages of the contracting process to deal with the risks associated with outsourcing IT services and complying with the FOIP Act and RMR.

2.2 JOINT SERVICE DELIVERY

It has been the practice for many years for various levels of government to cooperate in the delivery of government programs. In the area of social benefits, for example, it is common for the provincial, federal and municipal governments to share in the delivery of services.

A more recent development has been the establishment of common service centres where citizens can obtain one-stop shopping for a particular program or sector (e.g., a business centre providing a number of services relating to economic development which originate from different levels of government but are offered through a single site).

There has also been movement of services from one level of government to another in order that services may be offered more efficiently and closer to the citizen.

These joint service delivery initiatives vary in approach and format. The business and program objectives that a public body wishes to accomplish through shared or joint service delivery will dictate the extent of control over pre-existing records and over any records created or obtained during the new service delivery process.

Regardless of the approach taken, it is important to include in the contract or agreement, the nature and extent of control that is contemplated. This determines the extent to which the FOIP Act and RMR will apply in particular circumstances, and what conditions and standards apply to the records.

Components of a Joint Service Delivery Contract or Agreement

If joint service delivery is contemplated, there should be a written contract among the joint service providers setting out the terms and conditions for the service, including responsibilities for access to information, protection of privacy and records management. These contracts or agreements should:

- state what generic types of records each party to the service contract is providing in order to deliver the service (this is important in establishing the concept of control because there may be several parties providing records);
- specify whether records transferred to another authority remain under the control of the provincial public body and, if so, that the FOIP Act and the RMR continue to apply to them;
- in cases of joint service agreements between two public bodies, state which public body has custody and control of the records and assumes responsibilities under the FOIP Act and RMR;

- state that any amendment to the types of records involved may only be made with the mutual consent of the parties involved and that a copy of any amendment will be provided to the Senior Records Officer (SRO) of the public body;
- establish all the administrative, technical, and physical requirements and safeguards needed to ensure good management and to protect the confidentiality of the records, including separate storage, if appropriate, in order to facilitate applying the RMR and the FOIP Act;
- indicate which records created or obtained through joint or shared service delivery are the property of the Government of Alberta and governed by the FOIP Act and the RMR;
- specify that no records under the control of the public body will be destroyed, disposed of, or transferred to the physical custody of any other jurisdiction without the written consent of the public body and the Alberta Records Management Committee;
- state that any requests for access to records under the control of the public body will be directed to the public body within a specified number of days for response, either for routine disclosure or for processing of a FOIP request;
- state that on receipt of a request for access to records under the control of the public body, the public body will, if it requires records from the other party, notify that party and the records will be provided within a specified number of days from the date of the notification;
- state that only the public body (or, in cases where the joint service delivery agreement involves two public bodies, which public body) has the power to determine whether or not a record will be disclosed;
- specify that records provided in response to a FOIP request will be returned to their source location; and
- state that when the contract ends all records belonging a public body will either be returned to the public body or be transferred to the custody and control of the other party after approval by the Alberta Records Management Committee.

Additional components for information sharing agreements in regard to personal information are contained in the *FOIP Guidelines and Practices* manual.[3]

2.3 PRIVATIZATION

In some instances, public bodies are choosing to stop delivering certain services and are transferring provision of these services to non-government bodies. This can happen through the government offering the private sector the opportunity to move into the service field, through employee buy-outs, the turning over of services to another level of government or to a non-profit organization, or a combination of all these approaches.

In these instances, the public body may continue to carry on an inspection or audit role, or undertake licensing and

[3] This manual is available on the FOIP web site at: www.gov.ab.ca/foip.

set standards of operation. However, the public body's control over records transferred to, or created in, a privatized service environment would normally end. The records would no longer be subject to the FOIP Act.

Components of Privatization Contracts

A contract that governs privatization of a service should:

- clearly define the records or functions the public body will maintain control of, and relinquish control over all other types of records created by or transferred to the private service provider;
  - include a records retention and disposition schedule for the alienation of records approved by the Alberta Records Management Committee which governs the transfer of records to the private service provider, and which may:
  - establish the retention periods for these records;
  - state that no disposal of the records may take place without the written approval of the public body; and
  - state that final disposition of records will be either permanent retention, and therefore transferred to the Provincial Archives of Alberta, or destruction.
  - (Note: The schedule should be authorized by the Alberta Records Management Committee before the contract is signed.)
  - indicate the extent of any limited control which the public body may retain over records transferred to the private service provider and the extent of control of future records;
  - establish the measures that the private service provider must take to protect personal information from unauthorized access, use, disclosure, data matching or linkage, or destruction while that personal information remains in its custody.

The Provincial Archives of Alberta should be consulted when a privatization contract affecting records is being negotiated. The Archives may establish a procedure for preserving any archival records.

The transfer of responsibility for collecting, managing, using and disclosing personal information from government to a private service provider can cause particular difficulties. For example, personal information may have been originally collected, used and disclosed under conditions that imposed statutory requirements on the public body to protect the privacy of the individuals involved with the service.

Privatization of the service to the private sector or to any organization not covered by the FOIP Act (or similar legislation) means that these protections are being taken away. This may lead to criticism from affected individuals and the public generally. Wherever possible, public bodies should negotiate a clause in the contract under which the new service provider agrees to substantially meet the privacy protection provisions under **Part 2** of the FOIP Act. For example:

> For the records and information possessed or obtained by the contractor in connection with or under this contract, except those records which are in the sole custody and control of the contractor, the contractor agrees to comply with a standard consistent with the *Freedom of Information and Protection of Privacy Act* when providing the services or carrying out the duties or other obligations of the contractor under this contract.

On January 1, 2004, private-sector companies will be required to comply with Alberta's *Personal Information Protection Act*[4] or the federal *Personal Information and Electronic Documents Act* depending upon where they are located. These acts require companies to protect the personal information of clients and customers.

After this date, it is unlikely that a public body would need to impose additional privacy obligations on a new service provider.

[4] For more information, visit www.psp.gov.ab.ca

Chapter 3
The RFP and Tendering Process

3.1 REQUESTS FOR PROPOSALS

Ensuring compliance with the FOIP Act and the Records Management Regulation should begin during the Request for Proposal (RFP) stage of the contracting process. By clearly stating the requirements related to access to information, protection of privacy and records management in the RFP, contract managers can ensure that:

- potential contractors understand their responsibilities, and
- the full cost of compliance is built into the proposal for goods or services.

This section of the guide discusses:

- what to include in the RFP so that the prospective contractors understand their responsibilities;
- what to include in the RFP so that it is clear how records produced in the contracting process will be handled so that they comply with the requirements of the FOIP Act; and
- releasing contracting documents in response to a FOIP request.

3.2 COMMUNICATING REQUIREMENTS TO CONTRACTORS

Identification of Records

The specific records which the contractor will be expected to create, obtain or maintain under a contract should be stated in an RFP or tender document including one required for operational and financial accountability purposes. This is essential for determining which records created or obtained by the contractor are in the *custody* or under the *control* of the public body.

Normally the records created by contractors in the course of administering their own businesses, such as their financial records and other internal administrative matters, are not under the control of the public body.

Records Management Practices

If record-keeping forms a major part of a contracting arrangement, the RFP or tender document should include it as an item to be assessed and evaluated by the public body. Requirements for record-keeping may well affect both cost and method of service delivery.

Any special conditions relating to the storage of records which may add to the contractor's costs should be identified. For instance, contractors should be advised if certain records will have to be stored separately from other business records to ensure protection against unauthorized access, collection, use, disclosure or disposal of personal information. Particulars concerning

retention periods and requirements relating to the final disposition of records should also be noted, since these may affect the contractor's costs.

Special security measures should be described. Restrictions on where records or data can be located, such as a limitation to locations within Alberta or Canada, should be noted.

Access to Information Practices

Prospective contractors responding to an RFP or tender should be informed of the responsibilities they will assume, if they are selected to fulfil the terms of the contract, when a public body receives a FOIP request. For example:

> The records specified in this (RFP or tender) as being required to be maintained by the contractor are governed by the access and privacy provisions of the *Freedom of Information and Protection of Privacy Act*. Should (name of public body) receive a request for any of these records that are in your custody, it would be your responsibility to provide the records, at your expense. You should provide them to (position title, name of the public body) within (number) calendar days from official notification by (name of the official).

Protection of Personal Information

In some contracts, the collection and handling of personal information constitutes part of the services to be provided. In these cases, the RFP should describe the privacy protection requirements that the contractor will be expected to observe. For example:

> The contractor will meet the standards set by the requirements of Part 2 of the *Freedom of Information and Protection of Privacy Act*, for all personal information the contractor has access to, collects or uses, discloses or destroys as a consequence of carrying out obligations under the contract.

However, if handling personal information is a major part of the services to be provided, you may ask prospective contractors to provide a plan or approach for meeting these statutory obligations. For example:

> The *Freedom of Information and Protection of Privacy Act* requires the protection of the privacy of individuals whose personal information may be involved in meeting contract requirements. Under Part 2 of the Act, the contractor will be required to protect the privacy of each individual's personal information accessible to the contractor or collected under this contract. The contractor must include in its response to this (RFP or tender document) a detailed plan describing measures to meet each of the following requirements, as applicable:
>
> - manner of collection;
> - notification of collection purposes;
> - methods to ensure accuracy;
> - controls over use of personal information;
> - controls over disclosure of personal information;
> - plans and controls for data matching and linkage;
> - the retention and disposal of personal information; and
> - systems and methods for the protection of personal information from unauthorized access, collection, use, disclosure or disposal.

3.3 COMPLYING WITH FOIP

To ensure that a contract complies with the FOIP Act, issues regarding access to information, protection of privacy and records management should be addressed in the RFP or tender document prepared by the public body.

Confidentiality of RFP or Tender Submissions

It is important to inform potential contractors that, because of the access provisions of the FOIP Act, complete confidentiality of any document cannot be guaranteed.

Those who submit documentation should not, however, be left with the impression that all their information will automatically be disclosed. Bidders should be informed that, if a FOIP request is made for documents they provided to the public body, a number of exceptions outlined in the Act may be applied, including **section 16** (third party business information), and **section 17** (unreasonable invasion of personal privacy).

The notice provision that applies in relation to these exceptions gives the prospective contractor an opportunity to comment on the disclosure of records before a decision on access is made. The bidder also has a right of appeal to the Information and Privacy Commissioner if there is disagreement with the public body on the application of the Act's exceptions to disclosure.

As well, bidders should be encouraged to identify any parts of their submissions which are provided in confidence. Entire documents should not be identified as confidential, but if the release of certain information would be harmful to the business interests of prospective contractors, this should be noted in the document itself or in a covering letter.

This would clearly establish the bidders' expectations about the documents, both to the public body and to the Information and Privacy Commissioner, should there be a review of the public body's refusal to disclose this information in response to a FOIP request.

The RFP or tender documents should contain a clause similar to the following:

> All documents submitted to (name of the public body) are governed by the access and privacy provisions of the *Freedom of Information and Protection of Privacy Act*. While this *Act* allows persons a right of access to records in the (public body's) custody or control, it also prohibits (name of the public body) from disclosing your personal information or confidential business information. This prohibition takes effect if disclosure would be significantly harmful to your business interests or would be an unreasonable invasion of your personal privacy as defined in sections 16 and 17 of the Act. Contractors are encouraged to identify those portions of their submissions which they are submitting in confidence and which, if revealed, would harm the business interests of the company.

The above statement will alert contractors to the fact that their information, once submitted, may be disclosed to an applicant if it is requested and the public body releases it in accordance with the FOIP Act.

In some cases, the public body may intend to make public the contract price details. If this is the case, the public body should make that clear in the RFP.

If it is the policy of the public body to make certain information relating to the contracting process routinely available, it is also good practice to inform potential bidders of this in advance. Such information might include the list of potential bidders who obtained the tender, the list of those who submitted a proposal and minutes of the bidders' meeting.

Rating and Evaluation Records

Specific reference should also be made in RFPs and similar documentation to the matter of ratings. It should be clearly stated that under normal circumstances contractor ratings will not be disclosed to third parties but will be released only to the contractor that they are about. For example:

> Assessment criteria and allocation formulas for this (RFP or tender document) are public information. Individual assessments of bidders are considered confidential and of interest to competitors or other bidders under this (RFP or tender document). Individual assessment information will be provided, upon request, to the submitter/bidder to whom it relates, and to others, only in accordance with the *Freedom of Information and Protection of Privacy Act.*

Personal Information About Contractor's Employees or Agents

In many cases, RFPs may require submitters to provide personal information about their employees, such as evaluations of their ability and work history. Therefore, a *notice* to collect personal information similar to the following should appear in the introductory section of RFP or tender documentation:

> The purpose of collecting the personal information that must be provided in this (RFP or tender document) is to enable (name of the public body) to ensure the accuracy and reliability of the proposal, to enable (name of the public body) to evaluate your response to this (RFP or tender document) and to fulfil other related program purposes of (name of the public body). Authority for this collection is (name of statute and section(s)). You may contact (name of the appropriate officer) at (address and phone number) if you have any questions about collecting information under this (RFP or tender document).

If the information will be used for other purposes, these uses must be described in the RFP or tender document.

Chapter 4

Negotiating and Managing the Contract

4.1 DRAFTING THE CONTRACT

The contract should contain the FOIP and records management requirements that were in the RFP or tender documents. Also, you may want to include clauses that allow you to monitor performance during the life of the contract to ensure compliance with the FOIP Act and the RMR.

This section of the guide presents sample contract clauses related to:

- records management,
- access to information,
- protection of privacy,
- indemnification and breach of contract, and
- ongoing management of the contract.

Note: The model contract clauses provided in this section are examples only. Please seek legal advice on any clauses to be employed in particular contracts.

Where "Minister" is used, it may be appropriate to replace it with the name of a corporate public body that is not headed by a "Minister." The word "agreement" or a similar term can be substituted for the word "contract."

4.2 RECORDS MANAGEMENT

You should carefully consider which records must be under the control of the public body and which records are not needed by the public body. The contract must clearly define the records that are under the control of the public body and how these records are to be managed over time.

The contractor should be required to manage records under the public body's control according to the policies established under the RMR. The public body's Senior Records Officer (SRO) should be involved in establishing terms and conditions in a contract for the management of records, in establishing retention periods for records and the conditions governing how records will be stored, disposed of or destroyed.

Where appropriate, contracts should specify:

- the types of information and records the contractor is expected to collect or create and maintain for the public body while performing the contract;
- the definition of a record as it is understood in the contract;
- the types of records transferred to the contractor;
- the conditions for maintaining these records (e.g., access, control, confidentiality and security, retention or disposition or destruction);
- the public body's rights of ownership or other control of the records;

- the records retention periods and the conditions governing the disposition of records, and
- the basis on which the public body will access records in the custody of the contractor for the purposes of monitoring the contractor's operations (e.g., on-site inspection or transfer of the records to the public body).

Records Created or Maintained

If a wide variety of records is to be created under the contract, consider defining them in the contract. For example:

> Under this contract, the contractor will create or obtain the following types of records (listing of types of records).

Definition of Records

Many contractors will not be aware of the broad definition of record under the FOIP Act and the RMR. It would be useful to include the definition in the contract. The following clause incorporates the definition from the FOIP Act:

> In this contract, record means a record of information in any form, including notes, images, audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records.

The contract may also specify the nature of the record.

Transfer of Records and Conditions of Management

In many contracts, custody of certain records may be transferred by the public body to the contractor. However, the public body may want to maintain control of the records. In such cases, the contract should identify the records that are transferred and any conditions on the management of the records. For example:

> Under this contract, the following records (listing of types of records) have been provided to the contractor and will be maintained in the same organization and under the same conditions as they have been maintained by (name of the public body).

Alternatively, the public body may append to the contract specific conditions or standards for records management. The contract might include a clause such as:

> Under this contract, the contractor will maintain all defined records in a usable, organized form according to any conditions or standards established by (name of the public body) and appended to this contract.

Segregation of Records

In some cases, especially where sensitive personal information is collected, created or used, you may require the contractor to maintain those records separately from other business records. For example:

> The contractor must keep separate from all its other records and databases all personal information transferred to it by (name of the public body) or collected or compiled under this contract.

Ownership of Records

The FOIP Act and the RMR apply to records in the custody or under the control of the public body but do not deal with ownership. However, most contracts for services will also stipulate ownership of information in records produced under the contract. This is one way for the public body to exert control over the records produced under the contract and to protect the government's investment.

Three examples of clauses that have been used in this regard are:

> The contractor acknowledges that all (or specific) documents, surveys, plans, reports, examinations, analysis, master plates for a final report, and any and all other materials related to the services provided under this contract are the property of the Minister. They must be given to the Minister immediately upon request or when the contract ends, whichever occurs first.
>
> **OR**
>
> All technical information, inventions, methods and processes conceived or developed or first actually reduced to practice in carrying out this contract are the property of the Minister and must be fully and properly disclosed in writing to the Minister by the contractor. The contractor may not, without the written consent of the Minister, divulge or use such technical information, inventions, methods or processes other than in carrying out the project.
>
> **OR**
>
> Unless otherwise indicated by the Minister in a notice, the copyright to all material prepared by the contractor under this contract belongs to the Government of Alberta. Such material is to be delivered to the Minister upon completion of the project or as otherwise specified in this contract.

Records not in the Custody of the Minister

In some cases, such as joint service agreements (with a private sector contractor) or an outsourcing agreement, it may be beneficial to specify the records that are not in the custody or under the control of the public body. For example:

> The following types of records are deemed to be the sole property and in the control and custody of the contractor: (listing of types of records).

A public body cannot evade its FOIP responsibilities by saying that it does not have custody or control of records. However, the clause above could be used to make it clear that business records of a contractor that are unrelated to the contract are not in the custody or control of the public body.

Access by the Public Body

The public body must ensure that it is able to maintain control over records that are required to fulfil its mandate during the contract. One method of doing this is to include a clause to ensure that the public body has a right to access the records at any time. For example:

> The contractor will provide the (types of records) to (name of the public body) according to the following schedule.
>
> **OR**
>
> The contractor will provide to (name of the public body), at the contractor's expense, any and all records required to be created, obtained and maintained under this contract within (number) calendar days of notification by (position title).

OR

The contractor will allow (name of the public body) to inspect or review the (types of records) at the request of (name of the public body) within (number) calendar days of notification by (position title)

Records Retention

The RMR requires the deputy head of a public body to ensure that there is a records retention and disposition schedule for all records under the control of the public body. This requirement applies to records in the custody of the contractor, but under control of the public body. The contract should contain a clause similar to the following:

The records required to be created, obtained and maintained for the Minister under this contract become and remain the property of (name of the public body) and are to be

EITHER

retained and disposed of according to the conditions of the attached records retention and disposition schedule.

OR

delivered to (name of the public body) at the contractor's expense.

OR

disposed of in accordance with the records retention and disposition schedule attached to the contract.

If a records retention clause is used in the contract, a complementary clause relating to transitory records should be included. For example:

In this contract, a transitory record means a record containing information of temporary value which does not have some future administrative, financial, legal, research, or historical value to the government. This would include such information as duplicate records, draft documents, working materials, publications, blank forms, and temporary notes that do not have long-term value.

Transitory records as defined under this contract may be disposed of when they are no longer required, unless (name of the public body) advises the contractor to retain certain transitory records because a FOIP request has been received. Destruction must be done according to all rules and regulations which are now or may hereafter be established by the Government of Alberta.

Notification Prior to Destruction

As a safeguard against unlawful destruction of records, you should consider whether notification of destruction (even when destruction is allowed under the contract) should be required. This notification would allow the public body to have assurances that only records that should be destroyed are destroyed, especially for contracts with a lengthy duration.

A contract clause similar to the following could be used to establish the notice requirement:

Despite the above specifications or retention period, the contractor must, except for transitory records, notify (position title, name of the public body) that the records are about to be destroyed according to the contract. The contractor must receive (name of the public body)'s prior written approval for destruction and notify (name of the public body) that destruction has taken place.

4.3 ACCESS TO INFORMATION

Even if the contract does not involve the collection or use of personal information for the public body, you will still need to consider the access provisions of the FOIP Act. To ensure that the public body can comply with the Act, you should consider including in the contract:

- a general clause stating that records under the custody or control of the public body are subject to the Act;
- a statement regarding offences and penalties for altering, falsifying, concealing or destroying records; and
- conditions of storage of information, including media format, data and file specification, disaster recovery and a business continuity plan.

General Clauses

A general clause pertaining to FOIP can be useful in setting the stage for subsequent, more detailed descriptions of the contractor's obligations. However, you should not rely exclusively on a general clause pertaining to FOIP as it is unlikely to be effective if a dispute arises. Therefore, the contract needs to deal with the details of what is required of the contractor.

Here is an example of a general clause that you might consider using as a way of establishing the application of the FOIP Act to the contract.

> The contractor acknowledges that the *Freedom of Information and Protection of Privacy Act* applies to all information and records relating to, or obtained, created or collected under this contract.

Responding to FOIP Requests

The records in the custody of a contractor may be the subject of a FOIP request if they are also under the control of the public body. It is important that the contract clearly state the responsibilities of both the public body and the contractor in dealing with access requests. For example:

> The records created or collected under this contract for (name of the public body) are subject to the access and privacy provisions of the *Freedom of Information and Protection of Privacy Act*. Should (name of the public body) receive a request for any of these records that are in your custody, it would be your responsibility to provide (copies of) the records, at your expense. You should provide them to (position title, name of the public body) within (number) of calendar days from official notification by (name of the official).

Offences and Penalties

Section 92(1) of the FOIP Act contains several offences and penalties. It is an offence to wilfully:

- alter, falsify or conceal any record or direct another person to do so, with the intent to evade a request for access to the record;
- destroy any records subject to FOIP with the intent to evade a request for access to the records;
- collect, use or disclose personal information in violation of **Part 2**; or
- gain or attempt to gain access to personal information in violation of the Act.

The penalty for these offences is a fine up to $10,000. Contracting documents should clearly state that destroying records to evade providing access to them is an offence under the FOIP Act. For example:

> The contractor acknowledges that section 92 of the *Freedom of Information and Protection of Privacy Act* specifies that a person who wilfully destroys any records which are governed by the Act with the intent to evade a request for access to records is guilty of an offence and is liable to a fine of not more than $10,000.

> The contractor acknowledges that section 92 of the *Freedom of Information and Protection of Privacy Act* specifies that a person who wilfully collects, uses or discloses personal information in violation of Part 2 of the Act or gains or attempts to gain access to such personal information in violation of the Act, is guilty of an offence and is liable to a fine of not more than $10,000.

4.4 PROTECTION OF PRIVACY

Under **Part 2** of the FOIP Act, the head of each public body must protect individual privacy by applying **sections 33 to 42** of the FOIP Act. Therefore, if the contract involves the collection, use or disclosure of personal information for a public body, you must ensure that contractors handling the personal information meet those privacy obligations.

If the duties of the contractor do not involve the collection, use or disclosure of any personal information for the public body, these sections of the FOIP Act will not be applicable to the contract, so you can skip to section 4.5 of this Guide.

Contracts must clearly state the requirements for collecting, compiling, ensuring the accuracy of, protecting, using, accessing, disclosing, correcting and disposing of personal information imposed by the FOIP Act on the public body and assumed by the contractor.

The FOIP Act states that personal information may be collected only when specific authority for the collection exists. Therefore, it is essential, before a contract is entered into, to make sure that the appropriate authority exists to collect and use the personal information in the ways intended in the project. This will normally be done by consulting with the Program Manager and FOIP Coordinator.

The obligations of the contractor to protect the privacy of personal information should be specifically stated in the contract. A project may not, however, involve all aspects of collection, use and disclosure of personal information. The contract should reflect only those aspects relevant to the project.

Records containing personal information that are created for the public body under a contract will be subject to the privacy provisions of the FOIP Act. You should consider including clauses that cover the following aspects of FOIP in the contract:

- conditions under which personal information may be collected, used or disclosed on behalf of the public body;

- practices related to the protection of privacy by employees and agents of the contractor;
- responsibilities for maintaining the accuracy and completeness of personal information and for correcting personal information;
- acceptable use and/or disclosure of personal information; and
- any limits or conditions related to data matching or linkage.

Definition of Personal Information

Contracts should include a definition of "personal information" under the FOIP Act. For example:

> In this contract, personal information has the same meaning as in section 1(n) of the *Freedom of Information and Protection of Privacy Act* and means recorded information about an identifiable individual in any form. The definition in section 1(n) of the Act is provided in attachment (name attachment) to this contract.

Responsibilities of Employees and Agents

The duty to protect personal information applies to everyone working under the contract. As a result, there may be a need to provide training to the contractor's employees about FOIP or a need for the contractor to set up special procedures to be followed to protect personal information.

Contractor's employees should have access to only that personal information required to do their jobs. The contract should contain a clause similar to the following:

> The contractor agrees to notify each employee, officer and other person who may see or obtain access to the personal information of the duties and obligations established by **Part 2** of the *Freedom of Information and Protection of Privacy Act* and any specific processes and duties specified in the contract.

Should a breach of personal privacy occur, the contractor should be required to notify the public body immediately. For example:

> The contractor is responsible for ensuring the complete compliance of its employees and agents with all terms and conditions related to protection of privacy. In the event that the contractor becomes aware of a breach of any of these terms or conditions, it must notify (name of the public body) immediately in writing and take all reasonable measures to prevent any further breaches of these terms or conditions.

Collection of Personal Information

Section 33 of the FOIP Act governs the purposes for which personal information may be collected. The contract should contain a clause similar to the following:

> The contractor may not collect personal information pursuant to this contract, for the public body, unless the collection is authorized under the contract or the public body authorizes the collection.

Section 34 of the FOIP Act states that personal information must be collected directly from the individual the information is about (except in limited circumstances identified in the Act) and that the individual must be advised of:

- the purpose of the collection;
- the legal authority for collection; and

- contact information for someone able to respond to questions.

The contract should include a clause similar to the following:

> When personal information is collected for the (name of the public body) the contractor must collect it directly from the individual the information is about and must inform the individual of:
> (a) the purpose for which the information is being collected as stated in clause ____ of this contract; and
> (b) the specific legal authority for the collection as stated in clause ____ of this contract; and
> (c) the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection as stated in clause ____ of the contract.

If the contractor will collect personal information indirectly from a third party, this authority should be stated in the contract. For example:

> The contractor is authorized to collect personal information about individuals from (the following third parties) under the authority of (cite appropriate paragraph of section 34(1) of the Act).

Accuracy and Completeness

If an individual's personal information will be used by a public body to make a decision that directly affects the individual, **section 35** of the FOIP Act requires the public body to make every effort to ensure the information is accurate and complete. If the contracted services require compliance with **section 35** of the FOIP Act, a clause similar to the following should be included in the contract:

> The contractor, its employees and agents will make every reasonable effort to ensure that personal information that is or is to be used to make a decision that directly affects an individual is both complete and accurate.

If relevant, specific conditions to ensure this should be stated. For example, the public body may supply the contractor with regular data updates and rely on the contractor to update its own records accordingly, to ensure accuracy and completeness.

Correction

Section 36 of the FOIP Act gives individuals the right to request a correction to personal information. If personal information is collected or maintained under the contract for the public body, you will want to ensure that the information is corrected if the public body has determined that a correction is necessary. You should consider including a clause similar to the following in the contract:

> The contractor acknowledges that individuals or their representatives have the right to request the Minister to correct personal information that the contractor, its employees and agents may have either received from the public body or collected or compiled about an individual. The contractor must undertake to make any corrections or annotation required by the Minister within 5 working days of receiving notice and direction to do so by (name of the public body).

Protection of Personal Information

If significant amounts of personal information are handled by the contractor, or particular standards are required, a description of the standards required of the contractor (e.g.,

information security plans) should be attached to the contract.

> The contractor must protect personal information in its custody by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal of personal information. Specific measures include (state specific measures for physical, personnel and information technology security).

Examples of such standards might be:

> Access to personal information in a form that identifies or could be used to identify the individual(s) to whom it relates will be limited to (specific names, if possible, of specific employees of the contractor).

> The contractor must ensure that, before allowing any employee to have access to any personal information, each person named or referred to above signs an undertaking of confidentiality. The agreement covers all personal information they may become aware of in carrying out this (contract or agreement). Agreements are to be maintained on file by the contractor for the duration of the contract and for three years after completion of the contract unless otherwise specified in writing by (name of the public body).

> Personal information will only be kept at the following address (specify). Security will be maintained through the following physical measures (e.g., locked cabinets, security zones, locked rooms and controlled access to the premises) and the following appropriate information technology security measures (e.g., controlled computer access, authentication of systems users, and communications security).

Use and Disclosure of Personal Information

Sections 39 to 42 of the FOIP Act govern the use and disclosure of personal information. Contracts should contain a clause similar to the following:

> The contractor must not, either directly or indirectly, use personal information collected or maintained for the public body except for the following purposes (state purposes) necessary for performing the services provided by the contractor under this contract. Any other uses for any purpose other than those stated in this contract must be authorized by the Minister in writing before the information is used. At the end of this contract, the contractor, its employees and agents must not use any personal information obtained, collected or compiled as a result of this contract for any purpose.
>
> **OR**
>
> The contractor must ensure that no use or disclosure may be made of the personal information obtained by or provided to the contractor for any purpose other than what is needed to carry out this contract unless the contractor has received the prior express written authorization for doing so from (name of the public body).

Management and Retention of Personal Information

In most circumstances, you will need to consider whether personal information should be segregated from other records the contractor possesses. The following is an example of a clause stipulating the segregation of personal information:

> The contractor must keep separate from all its other records and databases all personal information transferred to it by (name of the public body) or collected or compiled under this contract.

Section 35(b) of the FOIP Act states that, where personal information is used by a public body to make a decision that

directly affects the individual, the public body must retain the personal information for at least one year after using it.[5]

Data Matching and Linkage

Some contracts may involve data matching as part of the contract. The contract should include a clause similar to the following:

> Data matching is the comparison of personal information obtained from different sources, including both electronic and paper-based formats, for the purpose of making decisions about the person to whom the data pertain. The contractor acknowledges that data matching and linkage forms part of the services under this contract. Data matching and linkage will comply with the policy direction stated in the ***Freedom of Information and Protection of Privacy Guidelines and Practices*** document, which is attached to this contract as (identify attachment).

4.5 HOLD HARMLESS

The contractor's responsibility for the protection of privacy and other terms of the contract continue after the conclusion of the work. A responsibility and indemnification clause should be included in all contracts. For example:

> The contractor agrees to hold harmless the Minister from any and all third party claims, demands, or actions for which the contractor is legally responsible, including those arising out of negligence, wilful harm, or crimes by the contractor or the contractor's employees or agents. This hold harmless shall survive this Agreement.

4.6 MONITORING COMPLIANCE

Section 38 of the FOIP Act specifically places a duty upon the head of a public body to protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, or destruction. Also, the public body must ensure that it is capable of responding to any FOIP request and to inquiries from the Information and Privacy Commissioner.

For this reason, you should consider setting up mechanisms to allow the public body to demonstrate that it is complying with the Act. The extent of these mechanisms will depend on the scope of the services covered by the contract and the duration of the contract.

Some mechanisms to consider are:

- regular requirements for the contractor to report on compliance, and
- on-site audits or evaluations of compliance.

There may also be a need to take remedial action during the life of the contract to correct deficiencies or to improve the public body's ability to comply with the FOIP Act and the RMR. One example of such action is to require the staff of the contractor to take FOIP training.

---

[5] The period may be shorter than one year if agreed to in writing by the individual, the public body and, if appropriate, the Alberta Records Management Committee.

Table 1
Methods of Dealing with Risk

Risk	RFP Clauses	Contract Clauses	Ongoing Management of Contract
Collection and Use	• Indicate FOIP requirements related to collection, use and disclosure	• Establish collection, use and disclosure criteria	• Have a mechanism for new collection and use • Provide FOIP training to staff collecting and using personal information
Custody and Control	• Identify who has custody and control of records created by the contractor	• Identify who has custody and control of specific records • Establish whether contractor can transfer data to others • Specify requirements of subcontractors • Establish procedures for orderly transition	• Monitor contract conditions are met
Records Storage and Access	• Assess financial viability • Specify any restrictions on location of records • Identify access requirements to records by public body	• Specify limitations on location of records • Establish public body rights to access data centres • Establish irrevocable right of access	• Review regular financial reports • Monitor contract conditions are met
Security	• Identify security requirements to safeguard paper and electronic records	• Specify security access procedures • Specify monitoring/audit procedures • Specify procedures relating to personnel replacement	• Monitor contract conditions are met, and audit security arrangements
Destruction of Records	• Reference Records Management Regulation • Specify penalties for wilful destruction	• Set out retention and disposition requirements	• Monitor contract conditions are met • Provide FOIP training to staff managing records
Sensitive Information	• Identify additional requirements as needed	• Specify any special requirements	• Monitor contract conditions are met • Provide FOIP training to staff handling sensitive information
Monitoring and Compliance	• Indicate reporting requirements	• Establish reporting requirements	• Analyze reports

Appendix 1

Glossary of Terms

Contracting is the process by which a public body enters into a contract enforceable in law where a legal obligation is defined between the government and another party or parties.

Control means that the public body has the authority to manage the record including restricting, regulating, and administering its use, disclosure and disposition. A public body will often exert control over records created under a contract even though the records may be in the possession of the contractor.

Custody means that the record is in the possession of the public body and the public body has a right to deal with the record and some responsibility for its care. It may be important for a public body to ensure continuity of custody over a record to meet legal requirements or to state clearly in a contract that this custody is being transferred to another party.

Disposition of records is the final handling of the records, either destruction or archival preservation, at the end of their life cycle.

Outsourcing is the process by which a public body enters into an agreement with another party (usually the private sector, but sometimes another public sector organization or non-profit organization) to deliver services or carry out operations on behalf of the public body. In these instances, the public body retains the responsibility for the service or the operation and may pay the other organization to carry out the government's responsibilities.

Joint service delivery involves an agreement among public bodies, different levels of government or non-profit organizations to join together in the delivery of programs and services which are related to one another but have been administered separately in the past.

Personal information is defined in **section 1(n)** of the FOIP Act as recorded information about an identifiable individual, including but not limited to:

- the individual's name, home or business address or home or business telephone number;
- the individual's race, national or ethnic origin, colour or religious or political beliefs or associations;
- the individual's age, sex, marital status or family status;
- an identifying number, symbol or other particular assigned to the individual;

- the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics;
- information about the individual's health and health care history, including information about a physical or mental disability;
- information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given;
- anyone else's opinions about the individual; and
- the individual's personal views or opinions, except if they are about someone else.

A **Privacy Impact Assessment** is the detailed consideration, during the planning and implementation of a program or system, of appropriate and effective measures to ensure compliance with Part 2 of the FOIP Act.

Privatization is the process by which a public body ceases to provide a service or carry out an operation and transfers the service or operation to the private or non-profit sector.

Public body, as used in this guide**,** is defined in **section 1(p)** of the FOIP Act. It includes, in part, a department, branch or office of the Government of Alberta as well as any agency that is listed in the FOIP Regulation and the offices of the Officers of the Legislature. Local public bodies are excluded.

Record is defined in **section 1(q)** of the FOIP Act as "recorded information in any form, and includes notes, images, audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers, papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records."

Transitory record means a record (as defined above) containing information of temporary value which does not have some future administrative, financial, legal, research, or historical value to the government. This would include such information as duplicate records, draft documents, working materials, publications, blank forms, and temporary notes that do not have long-term value.

Appendix 2

Checklist for Contract Managers

Planning

- ☐ How does this contract fit into the business and operational plans of the program involved? Is this a project requiring extensive control over the records of the contractor? What records will be required for accountability?
- ☐ What operational records will the contractor be expected to collect, create or maintain?
- ☐ If the contract involves the collection of personal information for the public body, what is the authority to collect that information?
- ☐ If the contract involves collection of personal information for the public body from third parties, is indirect collection for the purpose of the contract authorized under the FOIP Act?
- ☐ Which specific privacy provisions of the FOIP Act are relevant to the project and need to be addressed in the RFP and contract?
- ☐ If the contract involves data matching, data linkage or data sharing by or for the public body, is a Privacy Impact Assessment needed?
- ☐ Has there been consultation with the Senior Records Officer (SRO) about required records retention periods?
- ☐ Does record-keeping form a major part of the proposed contract that needs to be evaluated?
- ☐ If the contract is for IT outsourcing, what risks need to be addressed in the contract?

The RFP

- ☐ Does the RFP include a notice, as required by the FOIP Act, stating the public body's authority to collect personal information contained in submissions (e.g., personal information about the contractor's employees)?
- ☐ Does the RFP state which specific records the contractor will be expected to collect, create, or maintain for the public body?
- ☐ Does the RFP specify what records will be required for operational and financial accountability?
- ☐ Does the RFP make it clear which records will be in the custody or under the control of the public body and which will remain in the custody or control of the contractor?
- ☐ Does the RFP identify any special conditions relating to the storage of records that may add to the contractor's costs?

- ☐ If special security measures or restrictions on the location of data are required, does the RFP specify what they are?
- ☐ Does the RFP include information on the responsibilities of the contractor in the event of a FOIP request for records that are subject to the FOIP Act?
- ☐ Does the RFP describe the privacy protection requirements that the contractor will be obliged to observe? Or, if handling personal information is a major part of the contract, does the RFP provide for the prospective contractor to submit a plan for addressing privacy protection requirements under the FOIP Act?
- ☐ Does the RFP inform potential contractors that absolute confidentiality cannot be guaranteed for any submission? Does it advise potential contractors to identify those parts of their submissions which they believe should be held in confidence?
- ☐ If it is intended to make contract prices public, is this stated in the RFP?
- ☐ Does the RFP include information on access to contractor ratings?
- ☐ If record-keeping forms a major part of the proposed contract, does the RFP include it as an item to be evaluated?

The Contract

- ☐ Does the contract specify the types of information and records the contractor is expected to collect or create and maintain? Does the contract define the terms "record" and "personal information"? If the contract involves a variety of record types, does the contract define those as well?
- ☐ Does the contract need to include a general clause stating that records created under the contract are subject to the FOIP Act, in addition to detailed clauses relating to matters of access to information and protection of privacy that are relevant to the specific contract?
- ☐ Does the contract state which records are transferred to the contractor and specify standards for their management, including general obligations under the FOIP Act and the RMR? Does the contract include specific conditions for maintaining the records?
- ☐ Does the contract specify which records of the contractor will be in the custody or under the control of the public body and which will be in the custody or control of the contractor?
- ☐ Does the contract specify a records retention and disposition schedule? Does the contract include conditions governing the disposition of records, including transitory records?
- ☐ Does the contract include a requirement for the contractor to provide notification of destruction to the public body?
- ☐ Does the contract identify the responsibilities of the contractor relating to requests for access under the Act?
- ☐ Does the contract include information on offences and penalties under the Act?

- ☐ Does the contract make it clear that the requirements of the Act apply to everyone working under the contract? Are requirements relating to employees of the contractor, such as FOIP training, included in the contract?
- ☐ If the contract involves personal information, does it specifically state the requirements of the Act with regard to all of the following that are relevant to the contract?
  - collection of personal information,
  - notice requirements for direct collection,
  - authority for indirect collection,
  - specific conditions for ensuring accuracy,
  - the right of an individual to request correction of his or her own personal information,
  - specific standards for the protection of personal information,
  - restrictions on the use and disclosure of personal information,
  - records retention periods,
  - final disposition of the records
- ☐ If the contract involves sensitive personal information, are the terms and conditions adequate in relation to the increased risks? Does the contract specify that the information must be segregated from the contractor's other business records?
- ☐ If data matching or data linkage is part of the contract, does the contract specify terms and conditions?
- ☐ If the contract is for joint service delivery, does the contract identify responsibilities in relation to records management, access to information and protection of privacy?
- ☐ If the contract governs privatization of services formerly delivered by government, does the contract clearly define the records over which the public body will retain control and those over which the public body will relinquish control? Does the contract include a records alienation schedule, authorized by the Alberta Records Management Committee, governing the transfer of records?
- ☐ If the contract relates to IT outsourcing, are technical, administrative and legal requirements related to continuing access to the information specified in the contract? Does the contract specify requirements for disaster recovery?
- ☐ Does the contract include clauses allowing the monitoring of performance to ensure compliance with the FOIP Act and the Records Management Regulation (RMR)?
- ☐ Does the contract specify terms of access by the public body for the purposes of monitoring the contractor's operations?

Appendix 3

Releasing Contracting Records in Response to a FOIP Request

When a request is received for information on the contracting process, you must consider whether the records may be released without a FOIP request or whether the requester should make a FOIP request. It is preferable that if records must be severed or consultations held with third parties, a FOIP request be required to ensure that the applicant or third parties have the appeal process available to them.

When a FOIP request is made an applicant has a right to all or part of the records that are responsive to the request subject to the exceptions in the Act.

There are two types of exceptions to disclosure under the Act – mandatory exceptions and discretionary exceptions. If a mandatory exception applies to the information, the public body has a duty to refuse access.

Discretionary exceptions are those where the public body chooses whether to apply the exception. This part of the guide provides general information about the exceptions under the Act. For a more complete discussion of applying these exceptions, you should consult Chapter 4 of the *FOIP Guidelines and Practices* manual.

Mandatory exceptions that may apply to information in contracting records include the following:

- Disclosure harmful to the business interests of a third party (**section 16**);
- Disclosure harmful to personal privacy (**section 17**); and
- Privileged legal information of another person (**section 27(2)**).

Discretionary exceptions that may relate to information in contracting records include the following:

- Confidential evaluations (**section 19**);
- Advice from officials (**section 24**);
- Disclosure harmful to economic or other interests of the government or a public body (**section 25**); and
- Legal privilege (**section 27**).

It is important to note that all of these exceptions, except solicitor-client privilege under **section 27(2)** of the Act, apply to information contained in a record and not the entire record. If the information can reasonably be severed from the record, **section 6(2)** of the Act gives the applicant a right of access to the remainder of the record.

Disclosure Harmful to the Business Interests of a Third Party (section 16)

Section 16(1) of the FOIP Act creates a mandatory exception for information which, if disclosed, would reveal trade secrets or commercial, financial, labour relations, scientific or technical information of a third party that is supplied either explicitly or implicitly in confidence. However, the exception only applies if the disclosure could reasonably be expected to:

- harm significantly the competitive position or interfere significantly with the negotiating position of the third party;
- result in similar information no longer being supplied to the public body when it is in the public interest that similar information continue to be supplied;
- result in undue financial loss or gain to any person or organizations; or
- reveal information supplied to, or the report of, an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or inquire into a labour relations dispute.

The Information and Privacy Commissioner has established that the public body must satisfy the following three-part test before applying **section 16** (*IPC Order 97-013*):

1. Does the information contain trade secrets or commercial, financial, labour relations, scientific or technical information of the third party?

What kind of information qualifies under the first part of the test? Trade secret is defined in **section 1(s)** of the Act as meaning information, including a formula, pattern, compilation, program, device, product, method, technique or process:

- that is used, or may be used, in business or for a commercial purpose;
- that derives independent economic value, actual or potential, from not being generally known to anyone who can obtain economic value from its disclosure or use;
- that is the subject of reasonable efforts to prevent it from becoming generally known; **and**
- the disclosure of which would result in significant harm or undue financial loss or gain.

The Information and Privacy Commissioner has stated that "commercial information" relates to the buying, selling, or exchange of merchandise or services (*IPC Orders 96-013* and *97-013*). This includes third party associations, past history, references and insurance policies, as well as pricing structures and business plans *(IPC Orders 96-013, 97-013, 99-008* and *2001-021*). An agreement between two business entities may also contain commercial information (*IPC Order 2001-019).*

The Commissioner has also stated that "financial information" relates to information regarding the monetary resources of the third party, such as the third party's financial capabilities, and assets and liabilities, past or present (*IPC Orders 96-018* and *2001-008*). Common examples are financial forecasts, investment strategies, budgets, and profit and loss statements.

"Labour relations information" includes relationships within and between workers, working groups and their organizations as well as managers, employers and their organizations (*IPC Order 2000-003*).

"Scientific information" is information exhibiting the principles or methods of science, and "technical information" is information relating to a particular subject, craft or technique (*IPC Order 2000-017*).

"Technical information" is information relating to a particular subject, craft or technique (*IPC Order 2000-017*). Examples are system design specifications and plans for an engineering project.

2. Is the information supplied, explicitly or implicitly in confidence?

The second part of the test relates to whether the information was supplied explicitly or implicitly in confidence. This issue has received considerable attention from the Information and Privacy Commissioner in recent years. The Commissioner has stated that in order to meet the requirements, the following two conditions must be satisfied:

- the information has to be originally supplied in confidence during the proposal or negotiation stage and then used relatively unaltered in the contract, and
- the information contained in the contract must allow an applicant to make accurate inferences about sensitive third party business information that would not, in itself, be disclosed under the Act (*IPC Orders 96-012* and *96-018*).

Section 16(1)(b) does not cover information that is generated jointly through negotiation with the public body (*IPC Order 96-013*), but may apply where the information supplied to the public body during negotiations remains relatively unchanged in the agreement or could be inferred from an agreement (*IPC Order 2000-005*).

If there is a specific provision in the RFP that states the information will be kept confidential, the Commissioner has considered this to be an explicit condition of confidentiality. The Commissioner has also stated that, if proposals are required to be submitted in sealed envelopes, confidentiality is implied. (*IPC Order 97-013*).

Financial or commercial information will also be seen as supplied by a third party in confidence if it is originally supplied to a public body in confidence and that public body then supplies the information in confidence to a second public body (*IPC Order 2001-008*).

The Commissioner has accepted, as evidence of intended confidentiality, statements by the prospective contractor in the proposal or the covering letter to a proposal that the information supplied is confidential (*IPC Order 96-013*).

The Commissioner has recommended that public bodies and private service providers contracting with public bodies ensure that their contracts state whether the parties intend the transaction to be confidential (*IPC Order 2000-009).*

3. Could disclosure be reasonably expected to harm significantly the competitive position of the third party or one of the other conditions identified in section 16(1)(c) of the Act?

The final part of the test requires evidence of the likelihood of one of the harms specified, that is, evidence that disclosure can be expected to:

- significantly harm the competitive position of the third party;
- interfere significantly with the negotiating position of the third party;
- result in information no longer being available; or
- result in undue financial loss or gain to any person or organization.

To meet the harms test, the Information and Privacy Commissioner has stated that the "evidence must demonstrate a probability of harm from disclosure and not just a well-intentioned but unjustifiably cautious approach to the avoidance of any risk whatsoever because of the sensitivity of the matters at issue" *(IPC Order 96-003*).

In addition, evidence must be provided concerning:

- the connection between disclosure of the specific information and the harm which is alleged,
- how the harm constitutes "damage" or "detriment" to the matter, and
- whether there is a reasonable expectation that the harm will occur *(IPC Order 96-003*).

Disclosure Harmful to Personal Privacy (section 17)

Section 17 of the FOIP Act protects the personal privacy of individuals whose personal information may be the subject of a FOIP request by someone else. The protection is provided through a mandatory exception for personal information if its release constitutes an unreasonable invasion of an individual's privacy.

Section 17(4) of the Act identifies types of personal information for which it is presumed that the disclosure would be an unreasonable invasion of an individual's privacy. In determining whether a disclosure of personal information constitutes an unreasonable invasion of personal privacy, the public body must consider all relevant circumstances, including those identified in **section 17(5)** of the Act.

Privileged Legal Information of Another Person (section 27(2))

Section 27(1) of the Act provides that a public body may refuse to disclose information:

- that is subject to any type of legal privilege, including solicitor-client privilege or parliamentary privilege;
- prepared by or for the Minister of Justice and Attorney General, or prepared by or for an agent or lawyer of the Minister or of a public body, in relation to a matter involving the provision of legal services; or
- in correspondence between the Minister of Justice and Attorney General, or an agent or lawyer of the Minister or of a public body, and any other person, in relation to a matter involving the provision of advice or other services by the agent or lawyer.

Section 27(2) goes on to state that a public body **must** refuse to disclose information that is subject of any type of legal privilege, including solicitor-client or parliamentary privilege, that relates to a person other than the public body.

If a record is subject to solicitor-client privilege, it means that the record is confidential and does not have to be disclosed (*IPC Order 96-017*). Note that severing does not apply to records that are subject to solicitor-client privilege. The privilege must be claimed for the entire record or not at all.

Confidential Evaluations (section 19)

Section 19 of the FOIP Act states that a public body may refuse to disclose to an applicant personal information that is evaluative or opinion material compiled for the purposes of determining the applicant's suitability, eligibility or qualifications for employment or for the awarding of government contracts or other benefits where the information is provided explicitly or implicitly in confidence.

The exception is discretionary. It applies to information that is supplied by the source of the evaluation or opinion and not for information compiled by the public body. For example, a verbatim transcription or a summary of a reference check for a potential contractor that is supplied in confidence may be excepted from disclosure. However, an analysis of the interview prepared by the public body would not be excepted under this section.

Section 19 applies only when an individual, or a representative acting on his or her behalf, is requesting personal information about him or herself.

Advice from Officials (section 24)

Section 24(1) of the FOIP Act states that a public body may refuse to disclose information if the disclosure could reasonably be expected to reveal:

- advice, proposals, recommendations, analyses or policy options developed by or for a public body or a member of the Executive Council;
- consultations or deliberations involving officers or employees of a public body, a member of Executive Council, or the staff of a member of the Executive Council;
- positions, plans, procedures, criteria or instructions developed for the

purpose of contractual or other negotiations by or on behalf of the Government of Alberta or a public body, or considerations that relate to these negotiations;
- plans relating to the management of personnel or the administration of a public body that have yet to be implemented;
- the contents of draft legislation, regulations and orders of members of the Executive Council or the Lieutenant Governor in Council;
- the contents of agendas or minutes of meetings of an agency, board, commission, corporation, office or other body that is public body, or
- information, including the proposed plans, policies or projects of a public body, the disclosure of which could reasonably be expected to result in disclosure of a pending policy or budgetary decision.

The exception is discretionary. In determining whether or not to invoke the exception, public bodies should use the following three-step process:

- determine whether the information requested falls within one of the classes of information to which the exception to disclosure may apply;
- if it does, then determine whether or not disclosure of the information can reasonably be expected to *reveal* the particular class of information involved; and
- exercise discretion as to whether or not to disclose the record or part of the record based on whether or not disclosure would affect similar advisory processes in the future.

If **section 24(1)** is found to apply, it is necessary then to consider **section 24(2)**, which states that the provision does not apply to certain information, for example, information that is 15 or more years old.

Section 24(1)(a) is the most commonly used exception. The IPC has interpreted this provision strictly and determined that the list of words after "advice" constitute examples of advice. If the information doesn't fall within **section 24(2),** you must consider the information in the light of the test set out by the IPC. The IPC created a three-part test for determining whether advice falls within the exception. The advice must be:

- sought or expected, or be part of the responsibility of a person giving it by virtue of that person's position;
- directed toward taking an action, including making a decision; and
- made to someone who can take or implement the action (*IPC Order 96-006*).

As well, the Commissioner has established that a statement of fact, without any direction toward action to be taken, does not qualify as advice under **section 24** (*IPC Order 97-007*).

Disclosure Harmful to Economic or Other Interests of the Government or a Public Body (section 25)

Section 25(1) of the FOIP Act states that a public body may refuse to disclose information if the disclosure could reasonably be expected to harm the economic interest of a public body

or the Government of Alberta or the ability of the government to manage the economy, including:

- trade secrets of a public body or the Government of Alberta (as defined in **section 1(s)**;
- financial, commercial, scientific, technical or other information in which a public body or the Government of Alberta has a proprietary interest or a right of use and that has, or is reasonably likely to have, monetary value;
- information the disclosure of which could reasonably be expected to result in financial loss to, prejudice the competitive position of, or interfere with contractual or other negotiations of the Government of Alberta or a public body; and
- scientific or technical information obtained through research by an employee of a public body, the disclosure of which could reasonable by expected to deprive the employee or public body of priority of publication.

Section 25(1) is a discretionary exception. It ensures that, where harm would result from disclosure, certain portions of the information may be withheld. The types of information noted in the section are illustrative only and may not cover all types of information that could reasonably be expected to cause harm to economic interests.

In substantiating this exception, the public body must, regardless of the type of information, show that the information could reasonably be expected to harm the economic interest of a public body of the Government of Alberta or the ability of the Government to manage the economy (*IPC Orders 96-013* and *96-016*).

The Information and Privacy Commissioner has determined that the test for "reasonable expectation of harm" is:

- there must be a clear and direct linkage between the disclosure of the specific information and the harm alleged;
- the disclosure must cause harm and not simply interference or inconvenience; and
- the likelihood of harm must be genuine and conceivable (*IPC Orders 96-016* and *97-005*).

In addition, the public body must demonstrate a probability of harm from disclosure and not just a well-intentioned but unjustifiably cautious approach to the avoidance of risk (*IPC Orders 96-003* and *98-005*).

Chapter 4 of the *FOIP Guidelines and Practices* manual provides a fuller explanation of exceptions to disclosure under the FOIP Act.

Appendix 4

Disclosure of Documents used in Contracting *

Document	Disclosure Policy		Potential Exceptions	Comments
	Routinely Available	FOIP Request Required		
Requisition	no	yes	s.24 Advice from officials s.25 Economic interests of government or public body	Definition of requisition sometimes differs among public bodies
Tender documents	yes	no	None	May be available for fee
Invitation to Quote (ITQ), tenders or Request for Proposal (RFP)	yes	no	None	Generally public documents
Bidders invited for ITQ and RFP	yes	no	None	Generally available to public
Bidders' meeting minutes	yes	no	None	
List of bidders who bid	yes	no		List of bidders available
Bids, proposals, tenders	no	yes	s.16 Third party business interests s.17 Disclosure harmful to personal privacy	Bottom line $ amounts should be released
Unit prices	not always	yes, when no routine release	s.25 Economic interests of government or public body s.16 Third party business interests	Withheld
Evaluation committee's notes, memos etc.	no	yes	s.16 Third party business interests s.17 Disclosure harmful to personal privacy s.19 Confidential evaluations s.24 Advice from officials	
Evaluation of each bid, proposal, tender	no	yes	s.16 Third party business interests s.17 Disclosure harmful to personal privacy s.19 Confidential evaluations s.24 Advice from officials	Own evaluation generally available to each bidder
Summary of all evaluations	no	yes	s.16 Third party business interests s.17 Disclosure harmful to personal privacy s.19 Confidential evaluations s.24 Advice from officials s.25 Economic interests of government or public body	
Negotiation information	no	yes	s.16 Third party business interests s.17 Disclosure harmful to personal privacy s.19 Confidential evaluations s.24 Advice from officials s.25 Economic interests of government or public body	
Recommendation to award	no	yes	s.24 Advice from officials	
Signed contract or purchase order	no	yes	s.16 Third party business interests s.17 Disclosure harmful to personal privacy s.25 Economic interests of government or public body	Generally disclosed with some severing
Bidder's correspondence and responses	no	yes	s.16 Third party business interests s.17 Disclosure harmful to personal privacy	Disclosed with severing

* NOTE: This chart is a guide showing the example of a typical case. As for all FOIP requests, a review of the particular records requested must be made.

Appendix 5

ALBERTA REGULATION 224/2001

Government Organization Act

RECORDS MANAGEMENT REGULATION

Table of Contents

Interpretation	1
Alberta Records Management Committee	2
Chair, vice-chair and secretary	3
Records management program	4
Evaluation of program	5
Approval of records retention and disposition schedules	6
Advice to the Minister	7
Archival appraisal	8
Departmental responsibility	9
Records retention and disposition schedule	10
Destruction of records	11
Repeal	12
Expiry	13

Schedule

Interpretation

1(1) In this Regulation,

(a) "Committee" means the Alberta Records Management Committee established under section 2(1);

(b) "department" has the meaning given to it in section 14 of Schedule 11 to the *Government Organization Act*;

(c) "deputy head", in respect of a department, means

(i) the chief officer of the department, or

(ii) if there is more than one chief officer of the department, the chief officer of that part of the department for which he or she is responsible;

(d) "Minister" means the Minister of Government Services;

(e) "record" has the meaning given to it in the *Freedom of Information and Protection of Privacy Act*;

(f) "Schedule" means Schedule 1 to the *Freedom of Information and Protection of Privacy Regulation* (AR 200/95).

(2) For the purposes of this Regulation, an agency, board, commission, corporation, office or other body listed in the Schedule is considered to be a department.

AR 224/2001 s1;251/2001

Alberta Records Management Committee

2(1) There is established the Alberta Records Management Committee consisting of the persons appointed as members under subsection (3).

(2) On the request of the Minister, nominations must be made in accordance with the following and submitted to the Minister:

(a) two people must be nominated by the Department of Government Services;

(b) one person must be nominated by the Provincial Archives of Alberta;

(c) one person must be nominated by the Department of Justice;

(d) one person must be nominated by the Department of Finance;

(e) one person must be nominated by the Alberta Corporate Service Centre;

(f) one person must be nominated by the Chief Information Officer of the Government.

(3) The Minister may appoint as members of the Committee

(a) the persons nominated in accordance with subsection (2), and

(b) any other persons the Minister considers appropriate.

(4) A person nominated under subsection (2)(c) may in writing designate an employee of the Government who is under the administration of the Minister of Justice and Attorney General to attend and act on behalf of the person at one or more meetings of the Committee.

Chair, vice-chair and secretary

3(1) The Minister must designate one of the persons nominated under section 2(2)(a) to act as the chair of the Committee and the other to act as the secretary of the Committee.

(2) The members of the Committee may choose a vice-chair from among themselves.

Records management program

4(1) The Minister is responsible for establishing a records management program.

(2) For the purpose of providing the details for the operation of the records management program, the Minister may establish, maintain and promote policies, standards and procedures for the creation, handling, control, organization, retention, maintenance, security, preservation, disposition, alienation and destruction of records in the custody or under the control of departments and for their transfer to the Provincial Archives of Alberta.

Evaluation of program

5 The Committee may evaluate the implementation of the records management program in each department.

Approval of records retention and disposition schedules

6(1) The Committee must approve a records retention and disposition schedule of a department before it is implemented in the department.

(2) The Committee may approve records retention and disposition schedules submitted by the secretary of the Committee that are to apply to all departments.

Advice to the Minister

7 The Committee may provide advice to the Minister relating to the policies, standards and procedures referred to in section 4(2).

Archival appraisal

8 The member of the Committee referred to in section 2(2)(b)

(a) must provide an archival appraisal of each records retention and disposition schedule submitted by a department, and

(b) may provide advice on archival concerns.

Departmental responsibility

9 The deputy head of a department must ensure that records in the custody or under the control of the department are managed in accordance with the policies, standards and procedures established under section 4(2).

Records retention and disposition schedule

10(1) The deputy head of a department must ensure that the department prepares records retention and disposition schedules for all records under the control of the department.

(2) The records retention and disposition schedule must

(a) describe the records under the control of the department,

(b) specify how long the department must keep the records,

(c) specify where the records must be kept,

(d) specify the format in which records must be stored, and

(e) describe what the final disposition of the records will be.

(3) The records retention and disposition schedule must be approved by the Committee before it is implemented in the department.

(4) Records may be disposed of only in accordance with the approved records retention and disposition schedule.

Destruction of records

11 The deputy head of a department must ensure that records are destroyed only in accordance with policies established under section 4(2).

Repeal

12 The *Records Management Regulation* (AR 57/95) is repealed.

Expiry

13 For the purpose of ensuring that this Regulation is reviewed for ongoing relevancy and necessity, with the option that it may be repassed in its present or an amended form following a review, this Regulation expires on March 31, 2006.

SCHEDULE

See the Gazette for the official version of this Regulation and for the text of the Schedule.